Adv. Appl. Clifford Algebras 25 (2015), 53–63

0188-7009/010053-11
published online June 10, 2014
DOI 10.1007/s00006-014-0466-0

Advances in Applied Clifford Algebras

An Algorithm for Fast Multiplication of Pauli Numbers

A. Cariow* and G. Cariowa

Abstract. In this paper we introduce an efficient algorithm for the multiplication of Pauli numbers. The direct multiplication of two Pauli numbers requires 64 real multiplications and 56 real additions. More effective solutions still do not exist. We show how to compute a product of the Pauli numbers with 24 conventional multiplications, 8 multiplications by 1/2 and 56 real additions.

Keywords. Pauli numbers, multiplication of Pauli numbers, fast algorithm, matrix notation.

1. Introduction

In resent years the Clifford algebras and hypernumbers [1] play an important role in several fields of data processing including digital signal and image processing [2, 3, 4], computer graphics and machine vision [5, 6, 7], telecommunications [8, 9] and in public key cryptography [10]. Previous studies indicate that the most popular hypernumbers are quaternions, biquaternions, octonions, and sedenions. Perhaps the less popular are the Pauli numbers [11]. This numbers are mostly used in solving various physical problems in field theory, electrodynamics, etc. Among other arithmetical operations in Clifford algebras, multiplication is the most time consuming one. The reason for this is, because the addition of N-dimensional Clifford numbers requires only N real additions, whereas the multiplication of these numbers already requires $N(N-1)$ real additions and N^2 real multiplication. It is easy to see that the increasing of dimensions of Clifford number increases the computational complexity of the multiplication. Therefore, reducing the computational complexity of the multiplication of Clifford numbers is an important scientific and engineering problem. Efficient algorithms for the multiplication of quaternions, octonions and sedenions already exist [12, 13, 14, 15]. No such

*Corresponding author.

algorithms for the multiplication of the Pauli numbers have been proposed. In this paper, an efficient algorithm for this purpose is suggested.

2. Formulation of the Problem

A Pauli number is defined as follows:

$$\varphi = a_0 + a_1 i_1 + a_2 i_2 + a_3 i_3 + a_4 i_{12} + a_5 i_{13} + a_6 i_{23} + a_7 i_{123}$$

where $\{a_i\}$, $i = 0, 1, \ldots, 7$ are real numbers, i_1, i_2, i_3 are the main imaginary units and $i_{12} = i_1 i_2$, $i_{13} = i_1 i_3$, $i_{23} = i_2 i_3$, $i_{123} = i_1 i_2 i_3$ are the remaining imaginary units whose products are defined by the following equations:

$$i_1^2 = i_2^2 = i_3^2 = 1,\ i_2 i_1 = -i_1 i_2,\ i_3 i_1 = -i_1 i_3,\ i_3 i_2 = -i_2 i_3.$$

The results of all possible products of the Pauli numbers imaginary units can be summarized in the table (1).

TABLE 1. The results of all possible products of the Pauli numbers imaginary units

$\times$	i_1	i_2	i_3	i_{12}	i_{13}	i_{23}	i_{123}
i_1	1	i_{12}	i_{13}	i_2	i_3	i_{123}	i_{23}
i_2	$-i_{12}$	1	i_{23}	$-i_1$	$-i_{123}$	i_3	$-i_{13}$
i_3	$-i_{13}$	$-i_{23}$	1	i_{123}	$-i_1$	$-i_2$	i_{12}
i_{12}	$-i_2$	i_1	i_{123}	-1	$-i_{23}$	i_{13}	$-i_3$
i_{13}	$-i_3$	$-i_{123}$	i_1	i_{23}	-1	$-i_{12}$	i_2
i_{23}	i_{123}	$-i_3$	i_2	$-i_{13}$	i_{12}	-1	$-i_1$
i_{123}	i_{23}	$-i_{13}$	i_{12}	$-i_3$	i_2	$-i_1$	-1

Suppose we want to compute the product of two Pauli numbers.

$$\varphi_3 = \varphi_1 \varphi_2,$$

where

$$\begin{aligned}
\varphi_1 &= x_0 + x_1 i_1 + x_2 i_2 + x_3 i_3 + x_4 i_{12} + x_5 i_{13} + x_6 i_{23} + x_7 i_{123},\\
\varphi_2 &= p_0 + p_1 i_1 + p_2 i_2 + p_3 i_3 + p_4 i_{12} + p_5 i_{13} + p_6 i_{23} + p_7 i_{123},\\
\varphi_3 &= y_0 + y_1 i_1 + y_2 i_2 + y_3 i_3 + y_4 i_{12} + y_5 i_{13} + y_6 i_{23} + y_7 i_{123}.
\end{aligned}$$

Then we have:

$$\begin{aligned}
\varphi_3 = {} & (x_0 p_0 + x_1 p_1 + x_2 p_2 + x_3 p_3 - x_4 p_4 - x_5 p_5 - x_6 p_6 - x_7 p_7)\\
& + (x_0 p_1 + x_1 p_0 - x_2 p_4 - x_3 p_5 + x_4 p_2 + x_5 p_3 - x_6 p_7 - x_7 p_6)\, i\\
& + (x_0 p_2 + x_1 p_4 + x_2 p_0 - x_3 p_6 - x_4 p_1 + x_5 p_7 + x_6 p_3 + x_7 p_5)\, j\\
& + (x_0 p_3 + x_1 p_5 + x_2 p_6 + x_3 p_0 - x_4 p_7 - x_5 p_1 - x_6 p_2 - x_7 p_4)\, k\\
& + (x_0 p_4 + x_1 p_2 - x_2 p_1 + x_3 p_7 + x_4 p_0 - x_5 p_6 + x_6 p_5 + x_7 p_3)\, ij\\
& + (x_0 p_5 + x_1 p_3 - x_2 p_7 - x_3 p_1 + x_4 p_6 + x_5 p_0 - x_6 p_4 - x_7 p_2)\, ik\\
& + (x_0 p_6 + x_1 p_7 + x_2 p_3 - x_3 p_2 - x_4 p_5 + x_5 p_4 + x_6 p_0 + x_7 p_1)\, jk\\
& + (x_0 p_7 + x_1 p_6 - x_2 p_5 + x_3 p_4 + x_4 p_3 - x_5 p_2 + x_6 p_1 + x_7 p_0)\, ijk.
\end{aligned}$$

We can write

$$\begin{aligned}
&x_0p_0 + x_1p_1 + x_2p_2 + x_3p_3 - x_4p_4 - x_5p_5 - x_6p_6 - x_7p_7 = y_0,\\
&x_0p_1 + x_1p_0 - x_2p_4 - x_3p_5 + x_4p_2 + x_5p_3 - x_6p_7 - x_7p_6 = y_1,\\
&x_0p_2 + x_1p_4 + x_2p_0 - x_3p_6 - x_4p_1 + x_5p_7 + x_6p_3 + x_7p_5 = y_2,\\
&x_0p_3 + x_1p_5 + x_2p_6 + x_3p_0 - x_4p_7 - x_5p_1 - x_6p_2 - x_7p_4 = y_3,\\
&x_0p_4 + x_1p_2 - x_2p_1 + x_3p_7 + x_4p_0 - x_5p_6 + x_6p_5 + x_7p_3 = y_4,\\
&x_0p_5 + x_1p_3 - x_2p_7 - x_3p_1 + x_4p_6 + x_5p_0 - x_6p_4 - x_7p_2 = y_5,\\
&x_0p_6 + x_1p_7 + x_2p_3 - x_3p_2 - x_4p_5 + x_5p_4 + x_6p_0 + x_7p_1 = y_6,\\
&x_0p_7 + x_1p_6 - x_2p_5 + x_3p_4 + x_4p_3 - x_5p_2 + x_6p_1 + x_7p_0 = y_7.
\end{aligned}$$

Using the matrix notation, we can rewrite the above relations as follows:

$$\mathbf{Y}_{8\times 1} = \mathbf{P}_8\mathbf{X}_{8\times 1}, \tag{2.1}$$

where

$$\mathbf{X}_{8\times 1} = [x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7]^{\mathrm{T}},\ \mathbf{Y}_{8\times 1} = [y_0, y_1, y_2, y_3, y_4, y_5, y_6, y_7]^{\mathrm{T}},$$

$$\mathbf{P}_8 = \left[\begin{array}{cccc:cccc}
p_0 & p_1 & p_2 & p_3 & -p_4 & -p_5 & -p_6 & -p_7\\
p_1 & p_0 & -p_4 & -p_5 & p_2 & p_3 & -p_7 & -p_6\\
p_2 & p_4 & p_0 & -p_6 & -p_1 & p_7 & p_3 & p_5\\
p_3 & p_5 & p_6 & p_0 & -p_7 & -p_1 & -p_2 & -p_4\\
\hdashline
p_4 & p_2 & -p_1 & p_7 & p_0 & -p_6 & p_5 & p_3\\
p_5 & p_3 & -p_7 & -p_1 & p_6 & p_0 & -p_4 & -p_2\\
p_6 & p_7 & p_3 & -p_2 & -p_5 & p_4 & p_0 & p_1\\
p_7 & p_6 & -p_5 & p_4 & p_3 & -p_2 & p_1 & p_0
\end{array}\right].$$

The direct multiplication of two Pauli requires 64 real multiplications and 56 real additions. We shall present the algorithm, which reduce arithmetical complexity to 24 conventional multiplications, 8 multiplications by 1/2 and 56 real additions.

3. The Algorithm

At first, we rearrange the rows of the matrix $\mathbf{P}_8$ in the following order {8, 5, 6, 2, 7, 3, 4, 1}. Next, we rearrange the columns of obtained matrix in the same manner. As a result, we obtain the following matrix:

$$\mathbf{P}_8^{'} = \left[\begin{array}{cccc:cccc}
p_0 & p_3 & -p_2 & p_6 & p_1 & -p_5 & p_4 & p_7\\
p_3 & p_0 & -p_6 & p_2 & p_5 & -p_1 & p_7 & p_4\\
-p_2 & p_6 & p_0 & p_3 & -p_4 & -p_7 & -p_1 & p_5\\
-p_6 & p_2 & p_3 & p_0 & -p_7 & -p_4 & -p_5 & p_1\\
\hdashline
p_1 & -p_5 & p_4 & p_7 & p_0 & p_3 & -p_2 & p_6\\
p_5 & -p_1 & p_7 & p_4 & p_3 & p_0 & -p_6 & p_2\\
-p_4 & -p_7 & -p_1 & p_5 & -p_2 & p_6 & p_0 & p_3\\
-p_7 & -p_4 & -p_5 & p_1 & -p_6 & p_2 & p_3 & p_0
\end{array}\right].$$

Then we can write

$$\mathbf{P}_8^{'} = \mathbf{\Gamma}_8\mathbf{P}_8\mathbf{\Gamma}_8 = \left[\begin{array}{c:c}
\mathbf{A}_4 & \mathbf{B}_4\\
\hdashline
\mathbf{B}_4 & \mathbf{A}_4
\end{array}\right],$$

where

$$\mathbf{\Gamma}_8 = \left[\begin{array}{cccc:cccc} & & & & & & & 1 \\ & & & & & & 1 & \\ & & & & & 1 & & \\ & & & 1 & & & & \\ \hdashline & & & & & & & 1 \\ & & 1 & & & & & \\ & & & 1 & & & & \\ 1 & & & & & & & \end{array}\right],$$

$$\mathbf{A}_4 = \left[\begin{array}{cccc} p_0 & p_3 & -p_2 & p_6 \\ p_3 & p_0 & -p_6 & p_2 \\ \hdashline -p_2 & p_6 & p_0 & p_3 \\ -p_6 & p_2 & p_3 & p_0 \end{array}\right], \quad \mathbf{B}_4 = \left[\begin{array}{cccc} p_1 & -p_5 & p_4 & p_7 \\ p_5 & -p_1 & p_7 & p_4 \\ \hdashline -p_4 & -p_7 & -p_1 & p_5 \\ -p_7 & -p_4 & -p_5 & p_1 \end{array}\right].$$

It is easily seen [15] that the matrix with this structure can be factorized, than the computational procedure for multiplication of the Pauli numbers can be represented as follows:

$$\mathbf{Y}_{8\times 1} = \mathbf{\Gamma}_8 \mathbf{W}_8^{(0)} \mathbf{D}_8^{(0)} \mathbf{W}_8^{(0)} \mathbf{\Gamma}_8 \mathbf{X}_{8\times 1} \tag{3.1}$$

where

$$\mathbf{W}_8^{(0)} = (\mathbf{H}_2 \otimes \mathbf{I}_4) = \left[\begin{array}{cccc:cccc} 1 & & & & 1 & & & \\ & 1 & & & & 1 & & \\ & & 1 & & & & 1 & \\ & & & 1 & & & & 1 \\ \hdashline 1 & & & & -1 & & & \\ & 1 & & & & -1 & & \\ & & 1 & & & & -1 & \\ & & & 1 & & & & -1 \end{array}\right],$$

$$\mathbf{D}_8^{(0)} = \frac{1}{2}(\mathbf{A}_4 + \mathbf{B}_4) \oplus \frac{1}{2}(\mathbf{A}_4 - \mathbf{B}_4),$$

$\mathbf{H}_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ – is the order 2 Hadamard matrix, $\mathbf{I}_N$ is the order N identity matrix, and "$\otimes$", "$\oplus$" – denote the Kronecker product and direct sum of two matrices respectively [16].

Indeed, it is easy to see that matrix $(\mathbf{A}_4 + \mathbf{B}_4)$ has the following structure:

$$\mathbf{A}_4 + \mathbf{B}_4 = \left[\begin{array}{cccc} p_0 + p_1 & p_3 - p_5 & -p_2 + p_4 & p_6 + p_7 \\ p_3 + p_5 & p_0 - p_1 & -p_6 + p_7 & p_2 + p_4 \\ \hdashline -p_2 - p_4 & p_6 - p_7 & p_0 - p_1 & p_3 - p_5 \\ -p_6 - p_7 & p_2 - p_4 & p_3 - p_5 & p_0 + p_1 \end{array}\right].$$

Let us permute third and fourth column, first and third column, second and fours column of this matrix. As a result, the columns of the matrix are arranged in the following order: {4, 3, 1, 2}. Then permute third and fourth

row. As a result, we obtain the following matrix:

$$\mathbf{\Gamma}_4^{(1)}\left(\mathbf{A}_4+\mathbf{B}_4\right)\mathbf{\Gamma}_4^{(0)}=\left[\begin{array}{cc:cc} p_6+p_7 & -p_2+p_4 & p_0+p_1 & p_3-p_5 \\ p_2+p_4 & -p_6+p_7 & p_3+p_5 & p_0-p_1 \\ \hdashline p_0+p_1 & p_3-p_5 & -p_6-p_7 & p_2-p_4 \\ p_3-p_5 & p_0-p_1 & -p_2-p_4 & p_6-p_7 \end{array}\right].$$

The resulting matrix has the following structure:

$$\mathbf{\Gamma}_4^{(1)}\left(\mathbf{A}_4+\mathbf{B}_4\right)\mathbf{\Gamma}_4^{(0)}=\left[\begin{array}{c:c} \mathbf{A}_2 & \mathbf{B}_2 \\ \hdashline \mathbf{B}_2 & -\mathbf{A}_2 \end{array}\right],$$

where

$$\mathbf{\Gamma}_4^{(1)}=\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & & 1 \\ & & 1 & \end{bmatrix},\ \mathbf{\Gamma}_4^{(0)}=\begin{bmatrix} & & & 1 \\ & & 1 & \\ 1 & & & \\ & 1 & & \end{bmatrix},$$

$$\mathbf{A}_2=\left[\begin{array}{c:c} p_6+p_7 & -p_2+p_4 \\ \hdashline p_2+p_4 & -p_6+p_7 \end{array}\right],\ \mathbf{B}_2=\left[\begin{array}{c:c} p_0+p_1 & p_3-p_5 \\ \hdashline p_3+p_5 & p_0-p_1 \end{array}\right].$$

As shown in [15], the matrix having such a structure can be factorized as follows:

$$\mathbf{\Gamma}_4^{(1)}\left(\mathbf{A}_4+\mathbf{B}_4\right)\mathbf{\Gamma}_4^{(0)}=\mathbf{\Gamma}_4^{(1)}\mathbf{T}_{4\times 6}\mathbf{D}_6^{(0)}\mathbf{T}_{6\times 4}\mathbf{\Gamma}_4^{(0)} \tag{3.2}$$

where

$$\mathbf{D}_6^{(0)}=\frac{1}{2}diag\left[\begin{array}{c} \mathbf{A}_2-\mathbf{B}_2 \\ \hdashline -\left(\mathbf{A}_2+\mathbf{B}_2\right) \\ \hdashline \mathbf{B}_2 \end{array}\right],$$

$$\mathbf{T}_{4\times 6}=\left[\begin{array}{c:c:c} 1 & 0 & 1 \\ \hdashline 0 & 1 & 1 \end{array}\right]\otimes\mathbf{I}_2=\left[\begin{array}{cc:cc:cc} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ \hdashline 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right],$$

$$\mathbf{T}_{6\times 4}=\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}\otimes\mathbf{I}_2=\left[\begin{array}{cc:cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hdashline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \hdashline 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right].$$

Now consider the matrix $\mathbf{A}_4-\mathbf{B}_4$.

$$\mathbf{A}_4-\mathbf{B}_4=\left[\begin{array}{cc:cc} p_0-p_1 & p_3+p_5 & -p_2-p_4 & p_6-p_7 \\ p_3-p_5 & p_0+p_1 & -p_6-p_7 & p_2-p_4 \\ \hdashline -p_2+p_4 & p_6+p_7 & p_0+p_1 & p_3-p_5 \\ -p_6+p_7 & p_2+p_4 & p_3+p_5 & p_0-p_1 \end{array}\right]$$

Perform a permutation of rows and columns of this matrix in the same manner as in the matrix $(\mathbf{A}_4 + \mathbf{B}_4)$. Then the resulting matrix assumes the form

$$\boldsymbol{\Gamma}_4^{(1)} (\mathbf{A}_4 - \mathbf{B}_4) \boldsymbol{\Gamma}_4^{(0)} = \left[\begin{array}{cc:cc} p_6 - p_7 & -p_2 - p_4 & p_0 - p_1 & p_3 + p_5 \\ p_2 - p_4 & -p_6 - p_7 & p_3 - p_5 & p_0 + p_1 \\ \hdashline p_0 - p_1 & p_3 + p_5 & -p_6 + p_7 & p_2 + p_4 \\ p_3 - p_5 & p_0 + p_1 & -p_2 + p_4 & p_6 + p_7 \end{array}\right] = \left[\begin{array}{c:c} \widetilde{\mathbf{A}}_2 & \widetilde{\mathbf{B}}_2 \\ \hdashline \widetilde{\mathbf{B}}_2 & -\widetilde{\mathbf{A}}_2 \end{array}\right],$$

$$\widetilde{\mathbf{A}}_2 = \left[\begin{array}{c:c} p_6 - p_7 & -p_2 - p_4 \\ \hdashline p_2 - p_4 & -p_6 - p_7 \end{array}\right], \ \widetilde{\mathbf{B}}_2 = \left[\begin{array}{c:c} p_0 - p_1 & p_3 + p_5 \\ \hdashline p_3 - p_5 & p_0 + p_1 \end{array}\right].$$

This matrix can be factorized in the same way as the previous matrix:

$$\boldsymbol{\Gamma}_4^{(1)} (\mathbf{A}_4 - \mathbf{B}_4) \boldsymbol{\Gamma}_4^{(0)} = \boldsymbol{\Gamma}_4^{(1)} \mathbf{T}_{4\times 6} \mathbf{D}_6^{(1)} \mathbf{T}_{6\times 4} \boldsymbol{\Gamma}_4^{(0)} \tag{3.3}$$

$$\mathbf{D}_6^{(1)} = \frac{1}{2} diag \left[\begin{array}{c} \widetilde{\mathbf{A}}_2 - \widetilde{\mathbf{B}}_2 \\ \hdashline -(\widetilde{\mathbf{A}}_2 + \widetilde{\mathbf{B}}_2) \\ \hdashline \widetilde{\mathbf{B}}_2 \end{array}\right].$$

Substituting (3.2) and (3.3) in (3.1) we can write:

$$\mathbf{Y}_{8\times 1} = \boldsymbol{\Gamma}_8 \mathbf{W}_8^{(0)} \boldsymbol{\Gamma}_8^{(1)} \mathbf{A}_{8\times 12} \mathbf{D}_{12} \mathbf{A}_{12\times 8} \boldsymbol{\Gamma}_8^{(0)} \mathbf{W}_8^{(0)} \boldsymbol{\Gamma}_8 \mathbf{X}_{8\times 1} \tag{3.4}$$

where

$$\mathbf{A}_{8\times 12} = \mathbf{I}_2 \otimes \mathbf{T}_{4\times 6}, \ \mathbf{A}_{12\times 8} = \mathbf{I}_2 \otimes \mathbf{T}_{6\times 4}, \ \boldsymbol{\Gamma}_8^{(0)} = \mathbf{I}_2 \otimes \boldsymbol{\Gamma}_4^{(0)},$$
$$\boldsymbol{\Gamma}_8^{(1)} = \mathbf{I}_2 \otimes \boldsymbol{\Gamma}_4^{(1)}, \ \mathbf{D}_{12} = \mathbf{D}_6^{(0)} \oplus \mathbf{D}_6^{(1)}.$$

Let us now consider the structure of the remaining submatrices and their factorization.

$$\mathbf{A}_2 - \mathbf{B}_2 = \left[\begin{array}{c:c} p_6 + p_7 - p_0 - p_1 & -p_2 + p_4 - p_3 + p_5 \\ \hdashline p_2 + p_4 - p_3 - p_5 & -p_6 + p_7 - p_0 + p_1 \end{array}\right]$$
$$= (\mathbf{1}_{1\times 2} \otimes \mathbf{I}_2) \mathbf{D}_4^{(0)} (\mathbf{I}_2 \otimes \mathbf{1}_{2\times 1}),$$
$$\mathbf{D}_4^{(0)} = diag (s_0, s_1, s_2, s_3),$$
$$-(\mathbf{A}_2 + \mathbf{B}_2) = -\left[\begin{array}{c:c} p_6 + p_7 + p_0 + p_1 & -p_2 + p_4 + p_3 - p_5 \\ \hdashline p_2 + p_4 + p_3 + p_5 & -p_6 + p_7 + p_0 - p_1 \end{array}\right]$$
$$= (\mathbf{1}_{1\times 2} \otimes \mathbf{I}_2) \mathbf{D}_4^{(1)} (\mathbf{I}_2 \otimes \mathbf{1}_{2\times 1}),$$
$$\mathbf{D}_4^{(1)} = diag (s_4, s_5, s_6, s_7),$$
$$\mathbf{B}_2 = \left[\begin{array}{c:c} p_0 + p_1 & p_3 - p_5 \\ \hdashline p_3 + p_5 & p_0 - p_1 \end{array}\right] = (\mathbf{1}_{1\times 2} \otimes \mathbf{I}_2) \mathbf{D}_4^{(2)} (\mathbf{I}_2 \otimes \mathbf{1}_{2\times 1}),$$
$$\mathbf{D}_4^{(2)} = diag (s_8, s_9, s_{10}, s_{11}),$$
$$\widetilde{\mathbf{A}}_2 - \widetilde{\mathbf{B}}_2 = \left[\begin{array}{c:c} p_6 - p_7 - p_0 + p_1 & -p_2 - p_4 - p_3 - p_5 \\ \hdashline p_2 - p_4 - p_3 + p_5 & -p_6 - p_7 - p_0 - p_1 \end{array}\right]$$
$$= (\mathbf{1}_{1\times 2} \otimes \mathbf{I}_2) \mathbf{D}_4^{(3)} (\mathbf{I}_2 \otimes \mathbf{1}_{2\times 1}),$$

$$\mathbf{D}_4^{(3)} = diag\left(s_{12}, s_{13}, s_{14}, s_{15}\right),$$

$$-\left(\widetilde{\mathbf{A}}_2 + \widetilde{\mathbf{B}}_2\right) = -\left[\begin{array}{c:c} p_6 - p_7 + p_0 - p_1 & -p_2 - p_4 + p_3 + p_5 \\ \hdashline p_2 - p_4 + p_3 - p_5 & -p_6 - p_7 + p_0 + p_1 \end{array}\right]$$

$$= \left(\mathbf{1}_{1\times 2} \otimes \mathbf{I}_2\right) \mathbf{D}_4^{(4)} \left(\mathbf{I}_2 \otimes \mathbf{1}_{2\times 1}\right),$$

$$\mathbf{D}_4^{(4)} = diag\left(s_{16}, s_{17}, s_{18}, s_{19}\right),$$

$$\widetilde{\mathbf{B}}_2 = \left[\begin{array}{c:c} p_0 - p_1 & p_3 + p_5 \\ \hdashline p_3 - p_5 & p_0 + p_1 \end{array}\right] = \left(\mathbf{1}_{1\times 2} \otimes \mathbf{I}_2\right) \mathbf{D}_4^{(5)} \left(\mathbf{I}_2 \otimes \mathbf{1}_{2\times 1}\right),$$

$$\mathbf{D}_4^{(5)} = diag\left(s_{20}, s_{21}, s_{22}, s_{23}\right),$$

where

$$s_0 = \frac{1}{2}\left(p_6 + p_7 - p_0 - p_1\right),\ s_1 = \frac{1}{2}\left(p_2 + p_4 - p_3 - p_5\right),$$

$$s_2 = \frac{1}{2}\left(-p_2 + p_4 - p_3 + p_5\right),\ s_3 = \frac{1}{2}\left(-p_6 + p_7 - p_0 + p_1\right),$$

$$s_4 = -\frac{1}{2}\left(p_6 + p_7 + p_0 + p_1\right),\ s_5 = -\frac{1}{2}\left(p_2 + p_4 + p_3 + p_5\right),$$

$$s_6 = \frac{1}{2}\left(p_2 - p_4 - p_3 + p_5\right),\ s_7 = \frac{1}{2}\left(p_6 - p_7 - p_0 + p_1\right),$$

$$s_8 = \frac{1}{2}\left(p_0 + p_1\right),\ s_9 = \frac{1}{2}\left(p_3 + p_5\right),\ s_{10} = \frac{1}{2}\left(p_3 - p_5\right),\ s_{11} = \frac{1}{2}\left(p_0 - p_1\right),$$

$$s_{12} = \frac{1}{2}\left(p_6 - p_7 - p_0 + p_1\right),\ s_{13} = \frac{1}{2}\left(p_2 - p_4 - p_3 + p_5\right),$$

$$s_{14} = \frac{1}{2}\left(-p_2 - p_4 - p_3 - p_5\right),\ s_{15} = \frac{1}{2}\left(-p_6 - p_7 - p_0 - p_1\right),$$

$$s_{16} = \frac{1}{2}\left(-p_6 + p_7 - p_0 + p_1\right),\ s_{17} = \frac{1}{2}\left(-p_2 + p_4 - p_3 + p_5\right),$$

$$s_{18} = \frac{1}{2}\left(p_2 + p_4 - p_3 - p_5\right),\ s_{19} = \frac{1}{2}\left(p_6 + p_7 - p_0 - p_1\right),$$

$$s_{20} = \frac{1}{2}\left(p_0 - p_1\right),\ s_{21} = \frac{1}{2}\left(p_3 - p_5\right),\ s_{22} = \frac{1}{2}\left(p_3 + p_5\right),\ s_{23} = \frac{1}{2}\left(p_0 + p_1\right),$$

and $\mathbf{1}_{N\times M}$ is an integer matrix consisting of all 1s. Combining partial decompositions in a single computational procedure we finally can write following:

$$\mathbf{Y}_{8\times 1} = \mathbf{\Gamma}_8 \mathbf{W}_8^{(0)} \mathbf{\Gamma}_8^{(1)} \mathbf{A}_{8\times 12} \mathbf{A}_{12\times 24} \mathbf{D}_{24} \mathbf{A}_{24\times 12} \mathbf{A}_{12\times 8} \mathbf{\Gamma}_8^{(0)} \mathbf{W}_8^{(0)} \mathbf{\Gamma}_8 \mathbf{X}_{8\times 1} \quad (3.5)$$

where

$$\mathbf{A}_{12\times 24} = \mathbf{I}_6 \otimes \left(\mathbf{1}_{1\times 2} \otimes \mathbf{I}_2\right),\ \mathbf{A}_{24\times 12} = \mathbf{I}_6 \otimes \left(\mathbf{I}_2 \otimes \mathbf{1}_{2\times 1}\right),$$

$$\mathbf{D}_{24} = \bigoplus_{l=0}^{5} \mathbf{D}_4^{(l)} = diag\left(s_0, s_1, \ldots, s_{23}\right).$$

It can be seen, that

$$s_0 = s_{19},\ s_1 = s_{18},\ s_2 = s_{17},\ s_3 = s_{16},\ s_4 = s_{15},\ s_5 = s_{14},\ s_6 = s_{13},$$

$$s_7 = s_{12},\ s_8 = s_{23},\ s_9 = s_{22},\ s_{10} = s_{21},\ s_{11} = s_{20}.$$

Then it is easy to see that elements $\{s_k\}$, $k = 0, 1, \ldots, 11$ can be calculated using the following vector-matrix procedure:

$$\mathbf{S}_{12\times 1} = \widetilde{\mathbf{A}}_{12\times 8} \mathbf{D}_8 \left[\mathbf{H}_2 \oplus \left(\mathbf{H}_2 \otimes \mathbf{I}_2\right) \oplus \mathbf{H}_2\right] \mathbf{P}_{8\times 1} \quad (3.6)$$

where

$$\mathbf{P}_{8\times 1} = [p_0, p_1, p_2, p_3, p_4, p_5, p_6, p_7]^{\mathrm{T}},$$

$$\mathbf{S}_{12\times 1} = [s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9, s_{10}, s_{11}]^{\mathrm{T}},\ \mathbf{D}_8 = \frac{1}{2}\mathbf{I}_8,$$

$$\widetilde{\mathbf{A}}_{12\times 8} = \begin{bmatrix} -1 & & & & & & 1 & \\ & & 1 & -1 & & & & \\ & & & & -1 & -1 & & \\ & -1 & & & & & & -1 \\ -1 & & & & & & -1 & \\ & & -1 & -1 & & & & \\ & & & & 1 & -1 & & \\ & -1 & & & & & & 1 \\ 1 & & & & & & & \\ & & & 1 & & & & \\ & & & & & 1 & & \\ & 1 & & & & & & \end{bmatrix}.$$

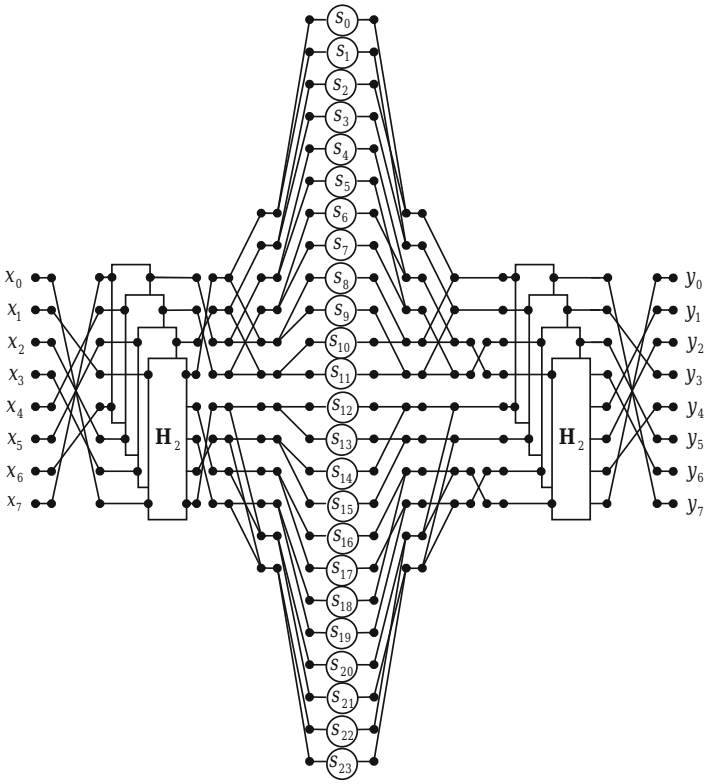

FIGURE 1. Data flow diagram for rationalized Pauli numbers multiplication algorithm

Fig. 1 shows a data flow diagram, which describes the fast algorithm for computation of the Pauli number product and Fig. 2 shows a data flow diagram of the process for calculating the vector $\mathbf{S}_{12\times 1}$ elements. In this paper, data flow diagrams are oriented from left to right. Straight lines in the figures denote the operations of data transfer. Points where lines converge denote summation. (The dash-dotted lines indicate the subtraction operation.) We deliberately use the usual lines without arrows on purpose, so as not to clutter the picture. The circles in these figures show the operation of multiplication by a variable (or constant) inscribed inside a circle. In turn, the rectangles indicate the matrixvector multiplications with the (2×2)-Hadamard matrices. As follows from Fig. 2, calculation of elements of diagonal matrix $\mathbf{D}_8$ requires performing only trivial multiplications by the power of two. Such operations may be implemented using common arithmetic shift operations, which have simple realization and hence may be neglected during computational complexity estimation [15].

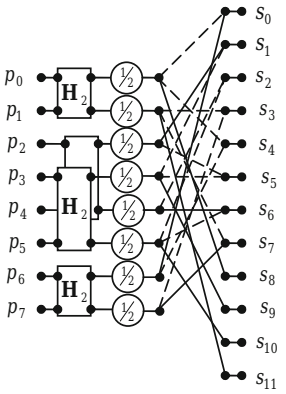

FIGURE 2. The data flow diagram describing the process of calculating elements of the vector $\mathbf{S}_{12\times 1}$ and in accordance with the procedure (3.6)

4. Conclusions

In this paper, we have presented an original algorithm allowing to multiply two Pauli numbers with reduced multiplicative complexity. As a result of streamlining the number of multiplications required to calculate the Pauli numbers product is reduced from 64 real multiplication to 24 conventional real multiplications and 8 multiplications by 1/2. Furthermore, the total number of arithmetic operations decreased by 32 compared with the naive method of calculations.

References

[1] R. Abłamowicz (ed.), *Clifford Algebras – Applications to Mathematics, Physics, and Engineering*. PIM 34, Birkhauser, Basel 2004.

[2] V. Labunets, *Clifford algebras as unified language for image processing and pattern recognition*. Computational Noncommutative Algebra and Applications, NATO Science Series II: Mathematics, Physics and Chemistry, volume 136 (2004), 197-225.

[3] J. Mennesson, Ch. Saint-Jean, L. Mascarilla, *A phase correlation for color images using Clifford algebra*. Applied Geometric Algebras in Computer Science and Engineering **9** (2010), 1-4.

[4] T. Batard, M. Berthier, and C. Saint-Jean. *Clifford Fourier transform for color image processing*. In E. Bayro-Corrochano and G. Scheuermann Eds, editors, *Geometric Algebra Computing in Engineering and Computer Science*. chapter 8, Springer Verlag 2010, pages 135-161.

[5] D. Hildenbrand , D. Fontijne , C. Perwass and L. Dorst, *Geometric Algebra and its Application to Computer Graphics*. Tutorial 3, in Proc. of 25th Annual Conference of the European Association for Computer Graphics, "Interacting with Virtual Worlds", Grenoble, France, INRIA and Eurographics Association, ISSN 1017-4656.

[6] J. Ebling and G. Scheuermann. *Clifford Fourier transform on vector fields*. IEEE Transactions on Visualization and Computer Graphics **11** (2005), 469-479.

[7] R. Wareham, J. Cameron, and J. Lasenby, *Applications of Conformal Geometric Algebra in Computer Vision and Graphics*. H. Li, P. J. Olver and G. Sommer (Eds.), IWMM 2004, LNCS 3519, (2005) 329-349.

[8] S. Karmakar, B. S. Rajan, *Multigroup Decodable STBCs From Clifford Algebras*. IEEE Transactions on Information Theory, vol. 55 No. 1 (2009), 223-231.

[9] M.Ye. Ilchenko, T.N. Narytnik, & R.M. Didkovsky, *Clifford algebra in multiple-access noise-signal communication systems*. Telecommunications and Radio Engineering, **72** (18) (2013), 1651-1663.

[10] E. Malekian, A. Zakerolhosseini and A. Mashatan, *QTRU: QuaternionicVersion of the NTRUPublic-Key Cryptosystems*. The ISC Int'l Journal of Information Security, vol. 3, No 1 (2011), 29-42.

[11] V. V. Silvestrov, *Number Systems*. Soros Educational Journal No 8 (1998), 121-127.

[12] O. M. Makarov, *An algorithm for the multiplication of two quaternions*. Zh. Vychisl. Mat. Mat. Fiz. **17** 6 (1977), 1574-1575.

[13] A. Cariow, G. Cariowa, *Algorithm for multiplying two octonions*. Radioelectronics and Communications Systems (Allerton Press, Inc. USA), vol. 55, Issue 10 (2012), 464-473.

[14] A. Cariow, G. Cariowa, *An algorithm for fast multiplication of sedenions*. Information Processing Letters **113** (2013), 324-331.

[15] A. Ţariov. *Algorithmic aspects of computing rationalization in digital signal processing* (in Polish), West Pomeranian University Press, 232, (2011).

[16] W. H. Steeb, Y. Hardy, *Matrix Calculus and Kronecker Product: A Practical Approach to Linear and Multilinear Algebra*. World Scientific Publishing Company; 2 edition, 324 pages (March 24, 2011).

A. Cariow and G. Cariowa
West Pomeranian University of Technology, Szczecin
Faculty of Computer Science and Information Technology
Żołnierska 49, 71-210 Szczecin
Poland
e-mail: atariov@wi.zut.edu.pl
gtariova@wi.zut.edu.pl

Received: January 8, 2014.
Accepted: April 7, 2014.